

THE STATE OF CYBERSECURITY FOR ACCOUNTING

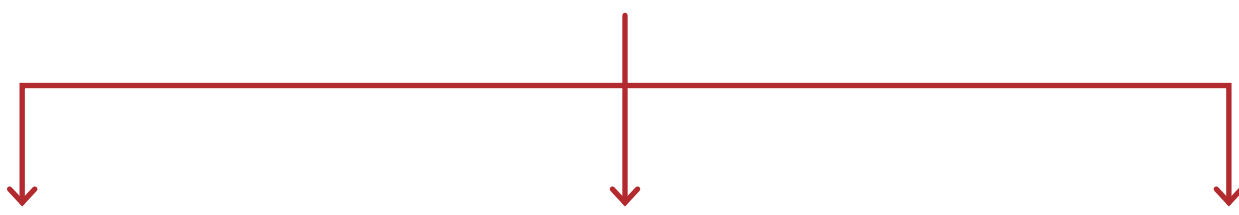
CLOUD COMPUTING HAS BEEN CALLED “THE FUTURE” OF THE ACCOUNTING AND TAX SERVICES INDUSTRY FOR MANY REASONS.

Firms can scale their server resources up and down as needed, have real-time access to applications and software, and even gain a competitive edge when clients are reassured that a firm’s enhanced cloud framework will protect their data.

However, since the accounting industry has grown to embrace digital transformation, they have long been in hackers’ crosshairs with no signs of slowing.



ACCOUNT NUMBERS, SOCIAL SECURITY NUMBERS, TAX INFORMATION—IT IS A VIRTUAL BUFFET OF SENSITIVE INFORMATION THAT PROVES TOO IRRESISTIBLE FOR HACKERS.



For accounting firm victims of ransomware, ransom amounts have generally ranged between \$100,000 for a small firm to \$2.6 million for a large firm.



Phishing scams remain the most popular way for cybercriminals to steal taxpayer information. Per the IRS, 91 percent of tax professional data breaches stem from employees opening an infected attachment of a legitimate looking email.



“Big Four” accounting giant Price Waterhouse Coopers estimates that financial institutions are over 30% more likely to be targeted than other businesses.

Want to learn more about how accounting firms can protect against cybersecurity threats? Read Armor’s “The State of Cybersecurity for Law, Accounting, and Financial Services” whitepaper.

DOWNLOAD